Aston University | CYBER SECURITY INNOVATION CSI CENTRE

Department for Digital, Culture, Media and Sport
Call for views on cyber security in supply chains and managed service providers
Aston Cyber Security Innovation (CSI) Centre
Response

About Aston

Aston Business School is in the top 1% of business schools worldwide with triple accreditation from AMBA, AACSB and EQUIS and has expertise in both cyber security and risk management, including regulation, governance and compliance. Aston University was ranked in the top 12 in the UK in all of its subject areas, with 86% of research undertaken was described as 'internationally significant'. Cybersecurity research is one of the priority areas for Aston Business School, which is evidenced by formation of the Cyber Security Innovation Research Centre in 2019.

Cyber Security Innovation (CSI) Centre brings together globally-recognised researchers delivering outcomes that have impact and address real-world cyber security challenges through innovative solutions. The scope of the Cyber Security Innovation Partnership is to effectively manage operations and build effective relationships across academia, industry and policy makers in the areas aligned with cyber security.

Lead by Professor Vladlena Benson, the CSI centre works with businesses to help improve their security posture and develops state of the art solutions for supply chain resilience and business continuity. Professor Benson has served on the UK Cyber Security Council formation project and has been a regular contributor to the policy formation dialogue with the Government on cyber security and emergent technologies.

Introduction

Aston Business School welcomes the initiative of the DCMS to address Supply Chain Security and frameworks underlining it. We support the Call for views in recognition that the evolving cyber security landscape requires new approaches to encourage organisations to increase efforts around management of suppliers and their accountability. In this space the role of the UK Government incentives and regulations is paramount in supporting businesses of all sizes and making the UK digital economy safe.

We support the Government efforts to bring Managed Service Providers into the conversation around their cyber security assurance reporting practices and transparency around their defence and incident handling mechanisms. This is of particular relevance in the aftermath of the most recent series of high profile cyber attacks on the MSPs (Kesya and SolarWinds), which had cascading consequences for their customers worldwide. There is an urgent need to address the lack of MSP accountability and assurance practices towards their client organisations, particularly SMEs, to enhance their cybersecurity posture.

Our recent research explored organisational approaches to supply chain management, specifically in the times of remote arrangements and when traditional business continuity

practices in supply chain management have been challenged. We base our response to the Call based on the evidence representing views of the ***West Midlands*** stakeholders.

Based on the conclusions of our research, we make a recommendation that cyber security of any organisation, inclusive of its supply chain, should be promoted in conjunction with other organisational targets, such as profitability, productivity and financial/operational risk management. The identification and promotion of synergies between Cyber security, profitability, and productivity is a strong driver to ensure that, at a senior level, organisations take responsibility and accountability for effective cyber risk management.

Indeed, profitability or productivity are close to the competitive advantage of the firm and security fo the supply chain of any organisation underpins its longevity on the market it operates in.

Investment in cybersecurity measures, including supply chain risk assessment and counter-threat controls, should be viewed as a **'cost of doing business'** and business success and/or longevity.

List of Questions

Part 1: Supply chain section

Questions on barriers to effective supplier risk management:
1.How much of a barrier do you think each of the following are to effective supplier cyber risk management?

a. Low recognition of supplier risk - **Severe barrier**

b. Limited visibility into supply chains - **Somewhat of a barrier**

c. Insufficient expertise to evaluate supplier cyber risk - **Somewhat of a barrier**

d. Insufficient tools or assurance mechanisms to evaluate supplier cyber risk - **Not a barrier**

e. Limitations to taking action due to structural imbalance - **Somewhat of a barrier**

2.Are there any additional barriers preventing organisations from effectively managing supplier cyber risk that have not been captured above?

○ Yes

3.[If Yes] What additional barriers preventing organisations from effectively managing their supplier risk are you aware of?

In the landscape of cybersecurity solutions developed mainly for large organisations (e.g. in features, budget, requiring deployment and operation skills), SMEs & MEs face significant challenges navigating the challenges of Digital Security, a complex issue that requires a specialised array of technical, business and managerial skills and the ability to effectively manage the interlinked domains of digital security, data and privacy.

Questions on supply chain cyber risk management

4.Have you used the NCSC's Supply Chain Security Guidance?

O Yes

5.How challenging do (or would) organisations find it to effectively act on these principles of supply chain cyber risk management, as outlined in the NCSC's Supply Chain Security Guidance?

a.Understanding the risks - **Not at all challenging**

b.Establishing control - **Not at all challenging**

c.Checking arrangements - **Slightly challenging**

d.Continuing to improve, evolve and maintain security - **Slightly challenging.**

6.What are examples of good practice for organisations implementing these aspects of supply chain cyber risk management?

- Open question

We particularly emphasise the need for point d. **Continuing to improve, evolve and maintain security**. The impact of a continuous, as opposed to one-off assessment, of supplier risk and having processes in place to maintain assurance of the supply chain entities.

Metrics for supplier assessment has been known to present difficulties. While supplier risk triaging may be well established for large organisations in the defence and highly regulated sectors, smaller organisations with a limited budget to undertake continuous cyber assurance processes and effectively setting metrics for ongoing use of controls may be disadvantaged.

Further, many organisations measure/express risk differently, and this process is gaining complexity when taking into account the multitude of regulations, standards, sector specific practices and international footprints are increasingly becoming a norm in the interconnected world of the digital economy.

7.What additional principles or advice should be included when considering supply chain cyber risk management?

- Open question

Through our research and work with the manufacturing community, we see a dire need to refocus the discussion on **hardware security standards** and regulation. For example, while the focal point of the recent regulatory developments including the GDPR aimed to address privacy and data protection, the cyber risks and business continuity are exacerbated by the security of hardware. With the IoT devices proliferating and enabling digital manufacturing supply chains the risk management practices must take into account hardware assurance levels.

As part of the Cyber Security Innovation Centre research projects on **Hardware Security by Design**, we conduct regular stakeholder roundtables. It has been highlighted on many occasions by SMEs and large manufacturers that security regulatory environment in dire need of change and innovation. Hardware security, inherently intertwined with software security, is defined by both national and international legislation and industry standards, and is predominantly reactive in nature. Moreover, this regulatory environment is characterised by insufficient awareness and driven by rudimentary assessments of cost and the path of least resistance. Its effectiveness is also hindered by contradictory regulations and the sub-standard agility of regulatory bodies in responding to emerging threats and industry trends. To reform hardware security regulations, there is a need for the harmonisation of standards and regulations, enhanced monitoring of information flows through the supply chains and expanding transactional monitoring capabilities, albeit conceding that some of these aspirations may be very complex to implement.

Questions on supplier assurance:

8.Have you used or do you plan to use the NCSC's Supplier Assurance Questions?

○ Yes

9.Since publishing the NCSC's Supplier Assurance Questions, it has been noted that the guidance could also cover the use of supplier-provided apps (e.g. where a supplier requires use of apps on an organisation's network to deliver its service to that organisation). Are there any additional areas of supplier assurance that should be outlined?

○ Yes

10.[If Yes] What additional areas of supplier assurance should be outlined?

Manufacturing is amongst the least protected sectors against cyber-crime, while the sector is now the third most targeted for attack. The 4th Industrial Revolution represents an

unprecedented opportunity for manufacturing through interconnectivity. However, the openness that interconnectivity implies, brings with it increased Cyber-risk. Cyber security in manufacturing is still characterised by specific and reactive interventions, while the nature of the threats and the importance of digitalisation urge for a cultural change, where Cyber security becomes integrated within the core activities of the firm, gaining the same importance and consideration of areas like quality management or occupational health and safety.

Questions on commercial offerings:
11.How effective are the following commercial offerings for managing a supplier's cyber risk?

a. Private supplier assurance - **Somewhat effective**

b. Platforms for supporting supplier risk - **Very effective**

c. Supply chain management system providers - **Somewhat effective**

d. Risk, supply chain and management consultancies - **Very effective**

e. Suppliers of outsourced procurement services - **Somewhat effective**

f. Industry cyber security certification schemes- **Very effective**

12.What additional commercial offerings, not listed above, are effective in supporting organisations with supplier risk management?

- Open question

- **Integration of cybersecurity risk management** as a part of enterprise wide operational risk management programme with the governance and accountability reaching to the top of the executive management.
- **Occupational Health and Safety and Cybersecurity** have similar ways of approaching in manufacturing. Both originate from the need of protecting the firm and its people from a set of risks. Therefore, both are based on a risk assessment process and on the definition of a set of mitigation action for the risks that are considered unacceptable. Moreover, both Occupational Safety and Cybersecurity require a participatory approach for their successful implementation, where the initiative of the management require active participation of all the workers and all the employees to be implemented successfully.

Question on additional government support:

13.How effective would the following government actions be in supporting and incentivising organisations to manage supply chain cyber risk?

a. Awareness raising of the importance of supply chain cyber risk management through the use of campaigns and industry engagement - **Very effective**

b. Additional support to help organisations to know what to do, such as:

- Improved or additional advice and guidance - **Very effective**
- A tool that draws on existing advice and standards to help organisations manage supplier cyber risk - **Very effective**

c. Providing a specific supplier risk management standard that:

- Outlines minimum and good practice and/ or - **Somewhat effective**
- Provides assurance that an organisation is managing their supply chain cyber risk - **Very effective**

d. Targeted funding to help stimulate innovation and grow commercial offerings that support organisations with their supplier risk management (e.g. Government competitions, accelerator programmes)

e. Regulation to make procuring organisations more responsible for their supplier risk management. - **Very effective**

f. Other (Please specify)

The rapid technological development in the digital and technology industry is both a blessing and a curse. Whilst enduring innovation provides a consistent stream of convenience-inducing technologies for consumers, regulatory bodies currently being outpaced by a significant margin. As the enactment of new legislation requires consensus across a wide variety of regulatory bodies, technology simply moves at a far greater pace than regulations can be enacted. With the emergent technologies presenting further risks, the IoT and cryptocurrency use are having a profound impact on supply chain risk. For example, there is no specific law for cryptocurrency in the UK, relying upon the Financial Services and Markets Act (2000) and other e-money regulations from 2011 to regulate the market. Resultantly, legislation of frequently outdated and consequently not fit for purpose.

Current legislation also promotes the perception of cyber security solely as **too complex** for the C-level management to understand and **as a cost**. On the other hand, cyber security has the potential of becoming an enabler for productivity, because of the visibility and control that it guarantees on the information flows within the firms and within the supply chains.

Turning cybersecurity from a cost centre to a productivity enabler requires an explicit recognition – also at a regulatory level – of the value creation potential of the information flows. The same regulatory mechanisms that facilitate the material flows across different regulatory systems should be put in place for information flows.

Response Compiled by:
Professor Vladlena Benson and Dr Donato Masi, Department of Operations and Information Management, Aston Business School. Birmingham, UK
csiresearch.co.uk

Contact Author: v.benson@aston.ac.uk

Publications used in this document:

- Saridakis, G., Georgellis, Y., **Benson, V**., Garcia, S., Johnstone, S., Lay, Y (2022) Work from Home (WFH), Employee Productivity and Wellbeing: Lessons from COVID-19 and Future Implications. Special Issue in *Information Technology & People (in press).*
- **Benson, V.** and Hughes, M (2019) *Building Business Resilience: What the Board of Directors Need to know. A Briefing for the C-Suite*. Information Systems Audit and Control Association, 2019. p 7.
- **Benson, V.** and McAlaney, J. (2019) *Emerging Cyber Threats and Cognitive Vulnerabilities*. Elsevier Cambridge, MA. p.394.
- Jones, N., **Benson, V.** and Danby, T. (2019) *Why don't organisations (communities) manage their cyber resilience well enough to remain trusted by stakeholders in the face of relentless cyber-attacks?* IAAC Workshop 3 Report, Aston University, November 11, 2019.